

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 Information associated with Nine Target Email
 Accounts more fully described in Attachment A.

Case No. **MJ23-083**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, attached hereto and incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

50 U.S.C. § 4819(a)(2)(f)

False statements to the Department of Commerce

18 U.S.C. § 1001

False statements

18 U.S.C. § 554

Smuggling

The application is based on these facts:

- ☒ See Affidavit of Special Agent Jose Rodriguez, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Jose Rodriguez, Special Agent
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date:

2/24/2023*Judge's signature*City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

I, Jose Rodriguez, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUNDS

1. I am a Special Agent with the U.S. Department of Commerce (DOC), Bureau of Industry and Security (“BIS”), Office of Export Enforcement (OEE) presently assigned to the Portland Resident Office in Portland, Oregon. I have been a Special Agent since July 2013 and I have worked for BIS since November 2009. I am a graduate of the Federal Law Enforcement Training Center’s Criminal Investigator Training Program and I have received training in the investigation of crimes related to the violation of export laws.

2. As a result of my training and experience, I am familiar with federal laws and regulations governing the export of goods and technology from the United States, including the International Emergency Economic Powers Act (50 U.S.C. §§ 1701–1706), the Export Control Reform Act of 2018 (50 U.S.C. §§ 4801–4852 (ECRA) and the Export Administration Regulations (15 C.F.R. pts. 730–774) (EAR).

3. I submit this affidavit in support of an application for a search warrant under 18 U.S.C. § 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 (hereinafter “Provider”) to provide information, including the content of communications, associated with **hans@khscm.be** (the “SUBJECT EMAIL ACCOUNT 1”), **hansdg@khscm.be** (the “SUBJECT EMAIL ACCOUNT 2”), **info@khscm.be** (the “SUBJECT EMAIL ACCOUNT 3”), **cp3350@hasainvest.be** (the “SUBJECT EMAIL ACCOUNT 4”); **hans@hasainvest.be** (the “SUBJECT EMAILACCOUNT 5”); **tom.degeetere@ett.be** (the “SUBJECT EMAIL ACCOUNT 6”); **kimb@khscm.be** (the “SUBJECT EMAIL ACCOUNT 7”); **rudi@khscm.be** (the “SUBJECT EMAIL ACCOUNT 8”);

double_mu2016@outlook.com (the “**SUBJECT EMAIL ACCOUNT 9**”) (collectively, the “**SUBJECT EMAIL ACCOUNTS**”), which are further described in Attachment A to this affidavit. As set forth below, I have probable cause to believe that the **SUBJECT EMAIL ACCOUNTS** contain evidence, as set forth in Attachment B to this affidavit, of violations of Export Control Reform Act 50 U.S.C. § 4819(a)(2)(A) (prohibited conduct), 50 U.S.C. § 4819(a)(2)(C) (attempt to violate the EAR), 50 U.S.C. § 4819(a)(2)(F) (false statements to the Department of Commerce), 18 U.S.C. § 1001 (false statements), and 18 U.S.C. § 554 (smuggling goods from the United States).

4. This affidavit concerns an investigation conducted by the U.S. Department of Commerce (DOC), Bureau of Industry and Security (BIS), Office of Export Enforcement (OEE). The statements contained in this affidavit are based on information I have learned through my personal participation in this investigation, from oral and written reports of other law enforcement officers, from records, documents, and other evidence obtained during this investigation, and from my experience and training as a Special Agent. Since this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the authorization of the search warrant.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated” and is also a court “in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored.” 18 U.S.C. § 2711(3)(A)(i), (ii).

6. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

7. This warrant application is to be presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

RELEVANT LAW

A. The Export Control Reform Act of 2018 (ECRA)

8. The ECRA provides, among its stated policy objectives, that “the national security and foreign policy of the United States require that the export, re-export, an in-country transfer of items, and specific activities of United States persons, wherever located, be controlled . . .” 50 U.S.C. § 4811(2). To that end, the ECRA grants the President the authority “(1) to control the export, re-export, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or by foreign persons; and (2) the activities of United States persons, wherever located, relating to” specific categories of items and information. 50 U.S.C. § 4812(b). The ECRA further grants the Secretary of Commerce the authority to establish the applicable regulatory framework.

9. Pursuant to ECRA, the DOC reviews and controls the export of certain items, including commodities, software, and technologies, from the United States to foreign countries through the Export Administration Regulations, 15 C.F.R. §§ 730-774. In particular, the EAR restrict the export of items that could make a significant contribution to the military potential of other nations or that could be detrimental to the foreign policy or national security of the United States. The EAR impose licensing and other requirements for items subject to the EAR to be lawfully exported from the United States.

10. The most sensitive items subject to EAR controls are identified on the Commerce Control List (CCL). 15 C.F.R. part 774, Supp. No. 1. Items on the CCL are categorized by an Export Control Classification Number based on their technical characteristics. Each Export Control Classification Number has export controls requirements depending on destination, end use, and end user. The Commerce Country

1 Chart identifies which exports require a license based on the reasons for control under the
2 relevant Export Control Classification Number and the country of destination.

3 11. Commodities that are not assigned a particular Export Control
4 Classification Number are designated as “EAR99.” Items designated as EAR99 require a
5 license for export to Cuba, Iran, North Korea, or Syria unless a license exception applies.
6 In addition, DOC maintains an Entity List (Supplement 4 to Part 744 of the EAR)
7 identifying persons and entities for which an export license is required, separate and apart
8 from license requirements arising from the Commerce Country Chart.

9 12. Under Title 50, United States Code Section 4819(a)(2)(A), no person may
10 engage in any conduct prohibited by or contrary to, or refrain from engaging in any
11 conduct required by this subchapter, the Export Administration Regulations, or any order,
12 license or authorization issued thereunder.

13 13. Under Title 50, United States Code Section 4819(a)(2)(C) no person may
14 solicit or attempt a violation of this subchapter, the Export Administration Regulations, or
15 any order, license or authorization issued thereunder.

16 14. Under Title 50, United States Code Section 4819(a)(2)(F), no person may
17 make any false or misleading representation, statement, or certification, or falsify or
18 conceal any material fact, to the Department of Commerce in the course of an action
19 subject to the EAR, or for the purpose of or in connection with effecting any export,
20 reexport, or in-country transfer of an item subject to the Export Administration
21 Regulations.

22 15. Under Title 50, United States Section 4819(b), “[a] person who willfully
23 commits, willfully attempts to commit, or willfully conspires to commit, or aids and abets
24 in the commission of, an unlawful act described in subsection (a),” shall be subject to
25 criminal penalties.

26 **B. Section 554**

27 16. Under Title 18, United States Code, Section 554, whoever fraudulently or
28 knowingly exports or sends from the United States, or attempts to export or send from the

United States, any merchandise, article, or object contrary to any law or regulation of the United States, or receives, conceals, buys, sells, or in any manner facilitates the transportation, concealment, or sale of such merchandise, article or object, prior to exportation, knowing the same to be intended for exportation contrary to any law or regulation of the United States, shall be fined under this title, imprisoned not more than 10 years, or both.

C. Section 1001

17. Under Title 18, United States Code, Section 1001(a), it is a crime to knowingly and willfully (1) falsify, conceal, or cover up by any trick, scheme, or device a material fact; (2) make any materially false, fictitious, or fraudulent statement or representation; or (3) make or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry.

SUMMARY OF PROBABLE CAUSE

A. Background Information on Hans De Geetere

18. De Geetere is a Belgium national and CEO/Owner of Knokke-Heist Support Corporation Management (KHSCM), located at Paul Parmentierlaan 121, 8300 Knokke Heist, Belgium. KHSCM provides supply chain management and procurement services for third parties. De Geetere is also currently named in a sealed indictment in the Eastern District of Texas (case number 19-cr-207). That indictment alleges that De Geetere violated 18 U.S.C. § 371 (Conspiracy to Smuggle Goods out of the United States in Violation of 18 U.S.C. § 554); 18 U.S.C. § 1956(h) (Conspiracy to Launder Monetary Instruments in Violation of 18 U.S.C. § 1956(a)(2)(A)); and 22 U.S.C. § 2778(b)(1)(A)(1) (Illegal Export of Defense Articles). In general, the indictment alleged that De Geetere conspired with others to facilitate the smuggling of electrical circuits to end users in China and Russia and to make or cause to make false and misleading statements to the producers of those circuits and to government officials that regulate their export.

B. The Accelerometers

1 19. The accelerometers discussed in this affidavit are manufactured by a
2 company in the Western District of Washington (the Manufacturer) and shipped from the
3 Western District of Washington. An accelerometer is a device that measures the
4 vibration, tilt, or acceleration of motion of a structure. They can be used in industrial
5 applications, but are also used frequently in aerospace and military systems. In aerospace
6 and military applications they play a critical role in structural testing and monitoring,
7 flight control systems, navigation systems, active vibration dampening, stabilization and
8 many other systems.

9 20. Pursuant to Section 15 of the Code of Federal Regulations, Part 744.21,
10 *Restrictions on certain 'military end use' or 'military end user' in Burma, The People's*
11 *Republic of China, The Russian Federation, or Venezuela*, in June 2018, the Deputy
12 Assistant Secretary of Commerce for Export Administration established a requirement
13 that exporters of these accelerometers obtain an export license in certain circumstances.
14 Initially, the requirement applied only to some exports to specific parties in China, but the
15 requirement was subsequently amended in December 2018 to cover all exports to China
16 and Hong Kong. The Manufacturer received a written notification of this requirement,
17 and the Manufacturer in turn informed its distributors and customers of the export license
18 requirement.

19 21. These accelerometers are designated EAR99 and, apart from the export-
20 license requirement just described, do not require a license to be exported to most
21 destinations. A license is required for export to embargoed countries such as Iran and
22 North Korea, or for prohibited end-uses or end-users, such as for use in ballistic missiles
23 in certain countries or by parties listed on the BIS Entity List. Based on my experience
24 investigating these type of export cases, Chinese companies are increasingly using
25 European companies to illicitly procure and divert U.S.-origin items because these
26 European companies are not subject to the same export control restrictions/requirements.

27 **C. Detention and Shipment Inspection**
28

1 22. On March 19, 2021, a representative from a company located in the
2 Western District of Washington (the Company), contacted OEE regarding an order of
3 concern. The order was for U.S.-origin accelerometers, and it was submitted by De
4 Geetere's company, KHSCM. KHSCM had submitted the order through a German
5 reseller of the U.S.-origin accelerometers, Delta Regeltechnik GmbH ("Delta"); the
6 German reseller Delta had in turn submitted the order to the Company to fulfill.

7 23. The Company shared documents with OEE that were provided to it by
8 Delta. In the documents, KHSCM claimed that the accelerometers were being ordered
9 for a Belgium government end-user, specifically Agentschap Wegen En verkeer,
10 Belgium. The documents submitted to Delta by KHSCM included an end-user form and
11 a document in Dutch, reportedly from a Belgium government agency "Departement
12 Buitenlandse Zaken," for the purchase of up to 20,000 accelerometers.

13 24. OEE consulted with the U.S. Department of Commerce's Frankfurt
14 Regional Export Control Officer about the authenticity of the KHSCM order. The
15 Frankfurt Export Control Officer advised that in 2018 his office completed a post-
16 shipment verification related to prior U.S. exports involving KHSCM. A "post-shipment
17 verification" is a process used to confirm the disposition of previously exported items
18 (often controlled items) and to confirm compliance with U.S export laws. The
19 verification process determined that KHSCM was an unreliable recipient of U.S.-origin
20 goods because, although KHSCM was the purchaser of the items subject to the 2018
21 post-shipment verification, those items were shipped to Sweden and eventually to Russia,
22 a final destination that was not disclosed to the Company, much less U.S. authorities,
23 thereby evading the requirement to obtain an export license. In addition, the Export
24 Control Officer advised that he had consulted with appropriate authorities in Belgium,
25 and that the information provided by KHSCM to Delta with respect to the accelerometer
26 shipment was likely false (i.e., Knokke-Heist was likely not, in fact, ordering the
27 accelerometers on behalf of the Belgian government).

1 25. On April 9, 2021, the Company shipped accelerometers for the KHSCM
2 order. As EAR99 items, these do not require an export license for Belgium. In
3 coordination with Customs and Border Protection (CBP), OEE detained the shipment for
4 inspection in order to try to establish the real end-user. OEE then contacted Delta
5 regarding the shipment and requested that a U.S. government form referred to as a BIS-
6 711 be completed. The BIS-711 form is entitled the "Statement by Ultimate Consignee
7 and Purchaser" and is designed to obtain a truthful statement about the ultimate end-user
8 of the goods being shipped. Delta provided to OEE a completed and signed BIS-711,
9 which claimed that Agentschap Wegen En verkeer, the Belgian company that KHSCM
10 had named as the end-user in its correspondence with Delta, was the Ultimate Consignee.
11 The form was purportedly signed by two individuals: "Dirk De Vroe", on behalf of
12 Agentschap Wegen En verkeer, and by "De Geetere H", referred to as the CEO of
13 Knokke-Heist. The BIS-711 form was dated April 15, 2021. The BIS-711 form reads in
14 relevant part, with respect to the signatories: "We acknowledge that the making of any
15 false statements or concealment of any material fact in connection with this statement
16 may result in imprisonment or fine, or both, and denial, in whole or in part, of
17 participation in U.S. exports and reexports."

18 26. An email message from Delta identified SUBJECT EMAIL ACCOUNT 1
19 as the email account used by De Geetere. Delta had terminated its business relationship
20 with De Geetere because they believed he was not being cooperative with the inspection
21 of the accelerometer shipment, and Delta then became suspicious. On May 3, 2021, De
22 Geetere wrote an email message, using the SUBJECT EMAIL ACCOUNT, directly to
23 the Company seeking to learn the status of the shipment. The Company referred De
24 Geetere to OEE, and I communicated with De Geetere directly at the SUBJECT EMAIL
25 ACCOUNT.

26 27. I arranged for a telephone call. I spoke with De Geetere by phone on May
27 12, 2021. I began the conversation by explaining that the U.S. Customs inspection of the
28 shipment had occurred because of the licensing requirement for exports to China and

1 Hong Kong of the accelerometers in the order. De Geetere responded, “Yes, I know, I
2 know.” I proceeded to discuss the documents De Geetere had provided to the Company
3 via Delta.

4 28. The first document we discussed was a letter dated February 16, 2021, from
5 KHSCM to Delta. De Geetere confirmed that the letter came from him. I asked about
6 the attachment (dated February 15, 2021) accompanying the letter, which, as noted
7 above, appeared to be an official document from the Belgian government. De Geetere
8 identified the attachment as a document from the Flemish Government, a regional
9 governmental entity within Belgium. I also asked about the BIS-711 that De Geetere had
10 signed, and asked specifically whether the other party identified on that form as the end-
11 user (Agentschap) was an integrator (e.g., a contractor or manufacturer that integrates the
12 accelerometers into a final product or component for specific end-uses) or the end-user of
13 the accelerometer. De Geetere identified Agentschap as the end-user, “the people who
14 signs for my projects.”

15 29. I asked De Geetere if he had customers outside Europe, specifically in
16 China, Hong Kong or the United Arab Emirates. De Geetere said no, and that he only
17 sells in Europe. De Geetere said the German reseller had asked him that many times, and
18 that he told them the same answer: no.

19 30. During the telephone conversation, De Geetere explained that the
20 accelerometers were not to satisfy any other company’s particular request, but were
21 rather ordered for a series of projects he was working on or identifying as part of a
22 “Corona Innovation fund” in Belgium. He described himself as an inventor, not as a
23 buyer and seller. I have been unable to locate any legitimate Belgian “Corona Innovation
24 fund” that matches the description he provided.

25 31. On May 17, 2021, I wrote to De Geetere, at SUBJECT EMAIL ACCOUNT
26 1, and informed him that I was not able to contact the individual who had signed the
27 BIS-711 with De Geetere (“Dirk De Vroe”) and that I would be advising the Company
28

1 not to continue with the order. I told De Geetere that if De Vroe contacted my office via
2 email or a phone call, we would reconsider. De Geetere asked for 48 hours.

3 32. On May 18, 2021, I received an email purportedly from De Vroe. De Vroe
4 copied the SUBJECT EMAIL ACCOUNT on the email message. De Vroe identified
5 himself as an official of Controle Strategische Goederen. De Vroe wrote:

6 33. "I can hereby confirm that the order the BV - KHSCM - with enclosed
7 reference letter KN0212807-KN (Paul Parmentierlaan 121 - 8300 Knokke Heist) is about
8 a project that is financed and purchased by our services. This concerns the current trial
9 order 81 pieces of [the Manufacture's accelerometers] and an open order that still needs
10 to be completed according to the needs of 20,000 pieces [the Manufacture's
11 accelerometers] (Year 2021)."

12 34. I contacted the Frankfurt Export Control Officer for further consultation.
13 On May 25, 2021, the Frankfurt ECO sent a message to Flemish Government officials,
14 who reviewed the communication from De Vroe and informed the Frankfurt Export
15 Control Officer that the end-user document was not, in fact, from the Belgian government
16 and that De Vroe's representations to U.S. authorities that he was acting on behalf of the
17 Belgian government entity were false. There was also no Dirk De Vroe at the Controle
18 Strategische Goederen office.

19 35. During my consultations with the Frankfurt Export Control Officer, he
20 further informed me that the Belgian authorities shared documents from a Belgian
21 customs inspection of one of De Geetere's previous shipments to Hong Kong, China. The
22 Belgian customs inspection took place around January 2021.

23 36. The January 2021 documents provided by Belgian officials show De
24 Geetere had mislabeled a package containing the Company's accelerometers as instead
25 containing LED parts. The packages were sent to Hong Kong. The Belgian government
26 documented the serial numbers; those serial numbers correspond to a prior order also
27 placed through Delta and satisfied by the Company. The documents for this order, which
28 was shipped on or around January 7, 2021, show that end user was KHSCM. At the time,

1 the Belgian authorities were not aware that the export of these accelerometers to China
2 was regulated by the United States, and the shipment was released after the paperwork
3 was corrected to accurately reflect the contents of the packages.

4 37. Eventually, communication between the parties regarding the shipment
5 detained by OEE ceased. OEE asked the Company to inform OEE if De Geetere ever
6 reached out to them again. During the following months, OEE uncovered that De Geetere
7 used unwitting parties in other countries or in the U.S. to purchase or try to purchase the
8 accelerometers on his behalf. In July 2021, CBP detained a shipment of accelerometers
9 that was being sent to a party in the United Arab Emirates (UAE), Yuttah FZE, that had
10 no prior history with significant exports of these items. I asked the UAE Export Control
11 Officer to visit the UAE recipient and confirm that the company was itself the end user of
12 these accelerometers, but the officer's inspection revealed that Yuttah's facilities did not
13 appear designed to use accelerometers in manufacturing; that Yuttah's facility lacked
14 specialized equipment necessary for integrating accelerometers into the products Yuttah
15 claimed to create; and that there were no visible, completed products of the type that
16 Yuttah's website advertised. Yuttah instead appeared to be a middleman for the large
17 accelerometer order it, a recently formed company, had placed. Yuttah's representative
18 also at first claimed that an employee who had corresponded with the Company was a
19 part-time sales representative, before later claiming (when pressed for proof of this
20 individual's existence) that they were a "virtual" sales representative. Forensic analysis
21 of the emails from the "virtual sales representative" and Yuttah's representative indicated
22 they came from the same digital device. Based on this circumstantial evidence of false
23 statements by Yuttah—including that it was not reshipping the accelerometers—
24 investigators obtained a search warrant to search the email account of the representative.
25 A review of that email account revealed that Yuttah's representative was in constant
26 contact with De Geetere, was ordering accelerometers on behalf of De Geetere, and was
27 receiving instruction from De Geetere on how to respond to Customs and Border
28 Protection/BIS.

1 38. In August 2021, in a separate incident, De Geetere attempted to place an
2 order via a third party in Florida. During the purchase order process, the Company
3 discovered De Geetere was behind the transaction when the Florida party submitted a
4 form with De Geetere listed as a contact for the end-user company. The Company
5 declined to complete the order.

6 39. In January 2021, a different third party in Florida placed an order for the
7 same type of accelerometers that De Geetere has been trying to procure. The general
8 language used for the description of the end-use was consistent with the language used by
9 De Geetere during prior attempts to purchase the accelerometers. This time, however, the
10 Florida party claimed the accelerometers were for domestic use. Special Agents from
11 BIS and Homeland Security attempted to contact the Florida party to discuss the order.
12 Subsequently, the Florida party appears to have stopped pursuing the order.

13 **D. De Geetere reengages with the Company**

14 40. On or around March 22, 2022, De Geetere approached the Company again
15 using SUBJECT EMAIL ACCOUNT 1. Once again, De Geetere claimed to be working
16 on a project for the Belgian government. This time, he requested a quote—meaning the
17 overall price he would have to pay—if he purchased 4000 accelerometers. The company
18 contacted OEE. De Geetere was eventually referred by the Company to an undercover
19 agent (UCA1) to pursue the transaction.

20 **E. False Statements to the Department of Commerce pursuant to a license**
21 **application**

22 41. During the negotiations with UCA1, De Geetere informed UCA1 that these
23 accelerometers were EAR99 and an export license was not required from U.S. regulatory
24 authorities to export them to Belgium. UCA1 offered to apply for an export license from
25 U.S. regulatory authorities to obtain a determination that a license was indeed not
26 required and avoid problems during shipping. On or around May 20, 2022, De Geetere,
27 using SUBJECT EMAIL ACCOUNT 1 responded in part “...I’m going to present your
28

1 *proposal with the government. But I suggest that as you say you apply for a permit. I*
 2 *think that's fair..."*

3 42. To facilitate UCA1 applying for a license, UCA1 obtained a BIS-711 form
 4 from De Geetere on or around May 5, 2022. This BIS-711 form identified the end-user
 5 as: "Vlaanderen Innovative, VAC Jacob Van Maerlantgebouw, Koning Albert 1-laan 1-2,
 6 Burgge 8200, Belgium." The official at that organization was identified in the form as
 7 "Dirk V". On or around May 27, 2022 the UCA1 business applied for the export license.

8 43. Based on the events surrounding the April 2021 detention, OEE has
 9 determined that De Geetere is not working on behalf of the Belgian government. OEE
 10 has not contacted the Belgian authorities again to confirm that the representations made
 11 on this BIS-711 form, including that the end user is a Belgian governmental organization,
 12 are false. According to open-source research, the address listed on the BIS-711 form
 13 (starting with "VAC Jacob Van ...") does appear to be the address of a Flemish
 14 governmental building. However, open-source research revealed no mention of an entity
 15 called "Vlaanderen Innovative." Moreover, on the May 5, 2022 BIS-711, the official
 16 listed for the Belgian organization is "Dirk V," while in the prior BIS-711 that Belgian
 17 officials confirmed were fraudulent, the signatory official purportedly working for the
 18 Belgian government was "Dirk De Vroe." As noted previously, Belgian officials
 19 confirmed in 2021 that no "Dirk De Vroe" worked for the Belgian authority listed in the
 20 May 18, 2021 email purportedly from a "Dirk De Vroe" to me.

21 **F. Information within SUBJECT EMAIL ACCOUNT 1**

22 44. Based on the facts articulated above, I obtained a warrant to search
 23 **SUBJECT EMAIL ACCOUNT 1** in this district (MJ22-297) on July 7, 2022. A review
 24 of records obtained pursuant to that search warrant identified multiple additional email
 25 accounts used by De Geetere, as well as potential coconspirators. The review also shows
 26 that De Geetere has multiple email accounts beyond what Provider hosts, and has
 27 incorporated multiple companies in various countries. The review also indicates that De
 28 Geetere appears to be purchasing on behalf of Russian companies and actively

1 corresponding with at least one publicly known Russian agent associated with Russian
2 intelligence services, as further discussed in paragraphs 62-64. In the paragraphs that
3 follow, I set forth relevant information about each of the SUBJECT EMAIL
4 ACCOUNTS that was obtained during my review of the records in SUBJECT EMAIL
5 ACCOUNT 1. The information set forth below establishes probable cause to believe that
6 the SUBJECT EMAIL ACCOUNTS contain evidence of violations of the statutes
7 identified in this affidavit.

8 45. *hansdg@khscm.be*, **SUBJECT EMAIL ACCOUNT 2**. Based on the
9 emails contained in SUBJECT EMAIL ACCOUNT 1, SUBJECT EMAIL ACCOUNT 2
10 appears to be used by De Geetere for administrative functions, but also appears to receive
11 quotes or inquiries from outside companies. For example, a Taiwan-based company
12 emailed a series of business inquiries to SUBJECT EMAIL ACCOUNT 2. . The email
13 text was formatted as a type of proposal form/business form. Part of the text of one such
14 email read "...We are able to buy..." followed by the commodity description and the
15 payment terms and instructions to the Taiwanese company. Because the Taiwanese
16 company is providing payment terms and instructions in exchange for purchasing the
17 specified commodity, the Taiwanese company will be engaging in the transaction on
18 behalf of the user of SUBJECT EMAIL ACCOUNT 2. The email text did not contain a
19 preceding text, but it contained a specific part number and quantity. Therefore, the
20 Taiwanese company must have received a request on a different email from SUBJECT
21 EMAIL ACCOUNT 2, a different email account or other form of communication like a
22 messaging app. Based on my experience investigating diversion of U.S. origin goods,
23 these inquiries were too specific to be unsolicited. Unsolicited emails related to buying or
24 selling electronic parts normally come with a wide list of parts attached to or a link to a
25 wider catalog. These inquiries extended from 2020 to 2022. Based on my experience, an
26 email relationship of that length would ordinarily indicate the Taiwanese company has an
27 established and ongoing business relationship with De Geetere.
28

46. For example, on September 8, 2021, the Taiwanese company sent to SUBJECT EMAIL ACCOUNT 2 an offer to buy 10,000 M29W640GT70NA6E integrated circuits for De Geetere. The email subject was "Inquiry 2021-09-08". The user of SUBJECT EMAIL ACCOUNT 1 then replies by changing the quantity from 10,000 to 9,000. Based on my review of this email, it appears that the Taiwanese company is responding to an inquiry from De Geetere with an offer to supply circuits, which De Geetere will then re-export elsewhere. These circuits are manufactured by a Massachusetts based company and classified by the manufacturer under ECCN 3A991. My review of the emails in SUBJECT EMAIL ACCOUNT 1 indicate a history of De Geetere shipping commodities to Hong Kong, China and Russia. Indeed, even when De Geetere exported to other European countries, the emails in SUBJECT EMAIL ACCOUNT 1 indicated it was typically to have those commodities re-shipped from the intermediate European country to a final destination in Hong Kong, China or Russia. Based on that lengthy practice, it is likely De Geetere was inquiring on behalf of customers based in Hong Kong, China or Russia. These circuits would require a license to be shipped if they were for military end-uses or end-users in China and Russia. In my experience, integrated circuits such as these are generally cheaper when purchased directly through the U.S. manufacturer or a U.S. base distributor. Based on my training and experience, I believe De Geetere may have inquired with the Taiwanese company in part to avoid export compliance screening and questions about the end-use and end-user from the U.S. parties. Because the sender is addressing SUBJECT EMAIL ACCOUNT 2, it is expected that SUBJECT EMAIL ACCOUNT 2 sent the original inquiry, and likely sent other such inquiries that might not be contained in SUBJECT EMAIL ACCOUNT 1. Therefore, based on my experience, I believe that additional evidence regarding illicit procurements is going to be found on SUBJECT EMAIL ACCOUNT 2.

47. info@khscm.be, **SUBJECT EMAIL ACCOUNT 3; and rudi@khscm.be, SUBJECT EMAIL ACCOUNT 8.** Based on the emails contained in SUBJECT EMAIL ACCOUNT 1, SUBJECT EMAIL ACCOUNT 8 appears to be managed by a "Rudi

1 Beun”. I personally confirmed with Belgium authorities that Rudi Beun is a natural
 2 Belgium person that works for De Geetere. On June 6, 2021, De Geetere received a
 3 Purchase Order from a Hong Kong-based company via SUBJECT EMAIL ACCOUNT 1.
 4 The order was for one hundred fifty (150) accelerometers. The phone number in the
 5 signature, “852-55159271,” appears to be related to the transaction discussed in
 6 paragraph 36. The user of SUBJECT EMAIL ACCOUNT 1 sent the order to SUBJECT
 7 EMAIL ACCOUNTS 3 and 8.

8 48. On June 4, 2021, the user of SUBJECT EMAIL ACCOUNT 8, emailed De
 9 Geetere with a payment confirmation for 17,305.88 Euros to Yuttah FZE. Those funds
 10 appeared to have been used by Yuttah to place the order for the accelerometers. Because
 11 the user of SUBJECT EMAIL ACCOUNT 8 is involved in payment processing and
 12 receiving invoices of transactions related to diversion of U.S. origin items—which, as
 13 explained above, there is probable cause to believe was in violation of U.S. export control
 14 laws—and SUBJECT EMAIL ACCOUNT 3 is copied on relevant emails, I believe more
 15 communications and documents constituting evidence of similar likely violations of U.S.
 16 export control laws will be found in SUBJECT EMAIL ACCOUNTS 3 and 8.

17 49. *cp3350@hasainvest.be*, **SUBJECT EMAIL ACCOUNT 4**. Based on the
 18 emails contained in SUBJECT EMAIL ACCOUNT 1, SUBJECT EMAIL ACCOUNT 4
 19 appears to be a network device such as a multifunction printer/scanner. An analysis of the
 20 firmware identified on a configuration page sent from SUBJECT EMAIL ACCOUNT 4
 21 to SUBJECT EMAIL ACCOUNT 1, led me to identify this device as a “bizhub C3350”
 22 manufactured by Konica Minolta. Konica Minolta’s website¹ identifies features that
 23 include cloud printing, among others. Cloud printing refers to the capability of sending a
 24 print (or a scan) directly to a storage device in the cloud, like OneDrive or Google Drive.

25 50. Based on my training and experience investigating individuals and small
 26 businesses purchasing and reselling goods, cloud storage is frequently used to store and
 27

28 ¹ <https://kmbs.konicaminolta.us/products/predecessor-products/bizhub-c3350/> accessed on February 15, 2023.

1 organize copies of sales and business documents. This is because, among other reasons,
2 cloud storage allows the use of folders and subfolders to organize documents by
3 transaction and are easily accessible from any computer, tablet, or mobile phone. In
4 addition, cloud storage mitigates the risk of loss of data due to loss, damage, or
5 malfunction of a hard drive or local storage device. A review of other emails from
6 SUBJECT EMAIL ACCOUNT 1 indicates that De Geetere has a OneDrive account with
7 5 terabytes of storage and appears to have a subscription to DropBox. For example, an
8 email sent by the user of SUBJECT EMAIL ACCOUNT 1, on July 27, 2021, to what
9 appears to be sent an external system administrator, translates with open-source
10 translation tools in part as: "... Do we also have a one drive on [SUBJECT EMAIL
11 ACCOUNT 1]? Can you also increase it to 5 TB?...". Another email sent by the user of
12 SUBJECT EMAIL ACCOUNT 8 on June 16, 2021, discusses the renewal of a DrobBox
13 Business account.

14 51. SUBJECT EMAIL ACCOUNT 4 appears to send regular emails to De
15 Geetere at SUBJECT EMAIL ACCOUNT 1. Based on my review of the emails, these
16 appear to be emails sent by De Geetere or his staff after scanning or printing business
17 documents. The emails include copies of invoices or purchaser orders for the
18 accelerometers subject to this investigation. For example, on May 24, 2022, SUBJECT
19 EMAIL ACCOUNT 4 sent SUBJECT EMAIL ACCOUNT 1 a file named
20 "SKM_C3350220524141200.pdf". This file identified another company, Eriner Limited,
21 Cyprus. Business information on the i-Cyprus (Cyprus Corporate Registry, www.i-cyprus.com)
22 identified Hans De Geetere as the Director of Eriner Limited. The file
23 included an invoice between Eriner and KHSCM for the types of accelerometers subject
24 to this investigation. SUBJECT EMAIL ACCOUNT 4 would thus likely contain the
25 same invoices and documents such as that one that appear in SUBJECT EMAIL
26 ACCOUNT 1—which themselves are evidence of the ongoing activity by De Geetere
27 discussed in this affidavit. But SUBJECT EMAIL ACCOUNT 4 might also contain
28 documents sent to other email addresses other than SUBJECT EMAIL ACCOUNT 1.

1 Moreover, SUBJECT EMAIL ACCOUNT 4 may contain emails received by, but then
2 deleted from SUBJECT EMAIL ACCOUNT 1, if those sent emails were not deleted in
3 SUBJECT EMAIL ACCOUNT 4. Finally, the emails sent to SUBJECT EMAIL
4 ACCOUNT 4, or data associated with that account, may reveal other co-conspirators or
5 employees working with De Geetere who employ the same printing or scanning function.

6 52. ***hans@hasainvest.be, SUBJECT EMAIL ACCOUNT 5.*** Based on the
7 emails contained in SUBJECT EMAIL ACCOUNT 1, SUBJECT EMAIL ACCOUNT 5
8 appears to be another email account likely operated by De Geetere and seemingly used
9 for communications like those in SUBJECT EMAIL ACCOUNT 1. As but one example
10 from the records contained in SUBJECT EMAIL ACCOUNT 1, on April 21, 2021, the
11 German reseller, Delta, sent an email to SUBJECT EMAIL ACCOUNT 5 regarding
12 order AU210346. In the email, there was a cancelation for the accelerometer order
13 discussed above in Section C. In other emails I reviewed, the signature block would
14 frequently have De Geetere's name, along with SUBJECT EMAIL ACCOUNT 5,
15 whether those emails were sent from SUBJECT EMAIL ACCOUNT 1 or SUBJECT
16 EMAIL ACCOUNT 5 (copying SUBJECT EMAIL ACCOUNT 1). In addition, it
17 appears likely that Delta used SUBJECT EMAIL ACCOUNT 5 to send an order
18 cancelation because they believed it was a valid point of contact for De Geetere, or
19 because De Geetere himself had transmitted the request to Delta using that account.
20 Therefore, it is likely that De Geetere or his associates use SUBJECT EMAIL
21 ACCOUNT 5 to create and send emails associated with the illicit procurement of
22 accelerometers and other transactions, as in at least this instance described above.

23 53. ***tom.degeetere@ett.be, SUBJECT EMAIL ACCOUNT 6.*** Based on the
24 emails contained in SUBJECT EMAIL ACCOUNT 1, SUBJECT EMAIL ACCOUNT 6
25 appears to be another email account that has regular communications with De Geetere
26 and likely contains communications like those in SUBJECT EMAIL ACCOUNT 1. On
27 January 21, 2021, the user of SUBJECT ACCOUNT 1 wrote an email to the user of
28 SUBJECT EMAIL ACCOUNT 6. I believe the user of SUBJECT EMAIL ACCOUNT 6

1 to be Tom De Geetere, who I understand is Hans De Geetere's brother based on
2 conversations with Belgium officials. When I accessed the domain ett.be it rendered to a
3 company called European Technical Trading. Tom De Geetere's LinkedIn profile
4 identifies him as the Managing Director of that entity. The January 21, 2021 email,
5 written in Dutch, which I translated informally using open-source translation tools,
6 appears to have been sent in response to a request for invoices to balance accounts
7 between the brothers' companies. The email had 12 invoices attached, one of the
8 attachments was an invoice 1/HDG/2019. Invoice 1/HDG/2019 identifies a transaction
9 billed by Karupini Holding BV to Foreign Trade Association Mashpriborintorg, Moscow,
10 a party on the BIS's Entity List. The invoicing party was Karupini Holding BV, a
11 Netherlands-based company. An email from SUBJECT ACCOUNT 1 to SUBJECT
12 EMAIL ACCOUNT 8, contains a signed document by De Geetere identifying him as the
13 Director for Karupini Holding BV. The signature is consistent with the signature on the
14 BIS-711 form discussed on paragraph 25. Mashpriborintorg was added to the Entity List
15 on March 2022, after this email was sent. Still, the January 21, 2021 email indicates that
16 De Geetere's operation is not solely for his benefit—in this email, for example, invoices
17 apparently placed by a company owned by De Geetere, were effected on behalf of his
18 brother's company. The email thread containing the invoices began with ETT explaining
19 the request. Using open source translation tools the translated thread reads in part as
20 follow:

21 *Hello Hans, In the appendix you will find 2 overviews of all invoices received*
22 *from KHSCM to Cippo and all payments from Cippo to KHSCM in 2020.*

23 *However, these do not match. There is a difference of 19,872.50 euros. Cippo has*
24 *received invoices for 88,342.80 euros and made payments for 108,215.30 euros.*

25 *Either Cippo has not received and entered all your invoices or has Cippo paid too*
26 *much?....*

27 Tom De Geetere's LinkedIn profile identify him as Owner and CEO of a company called
28 Cippo. Based on the text written by the ETT employee, it appears that Cippo is used in

1 part to pay invoices between the companies. Cippo's physical address appears to be a
 2 residential address: Jsbeerlaan 7, 9850 Deinze, Belgium. I did not find a website for the
 3 company. However, some of the attached invoices correspond to brands ETT sells on
 4 their website, <https://www.ett.be/> . For example, invoice 04/KH/2020, as translated by
 5 open-source software, reads in part:

6 *Support IC source customers USA – HL Intel, Memory, Apple, SSD Investigate credit*
 7 *insurance payment options.*

8 This invoice was from Knokke Heist Support Corporation Management to Cippo.

9 54. It also appears that De Geetere is still actively using Karupini or the
 10 business relationships associated with the company to procure U.S.-origin goods on
 11 behalf of Russian parties in a manner designed to avoid export controls and sanctions.
 12 For example, an email sent to SUBJECT EMAIL ACCOUNT 1, in May 2021, suggest
 13 De Geetere re-entered into an agreement with Russian parties to procure U.S.-origin
 14 goods. The agreement reads in part:

15 *... The Assignor has agreed in the normal course of business about the supply*
 16 *of special-purpose goods (several US-made kinds of microchips) by Karupini*
 17 *Holding BV (Netherlands) and from July 2016 to December 2017 was making*
 18 *advance payments to the bank account of Karupini Holding BV for the delivery*
 19 *of goods for the total amount of 3 448 416.00 (Three million four hundred forty-*
 20 *eight thousand four hundred sixteen) euros 52 cents;*

21 ...

22 *The Parties wish to enter into the present Agreement for the assignment by the*
 23 *Assignor to the Assignee of all rights and obligations arising from the prepaid*
 24 *delivery of goods to be supplied by Karupini Holding BV to the Assignor and the*
 25 *resulting Debt of Karupini Holding BV to the Assignor.*

26 The Assignor is ORIENTAL TRADING INCORPORATED. According to the contract
 27 Oriental trading is a company organized and operating under the laws of the United Arab
 28

1 Emirates and at its registered address at JLT, Swiss Tower, 204-B, DUBAI, UAE, P. O.
2 Box 309073 , and signing for the Assignor is a person named Stanislav Romanyuk.

3 55. Based on my training and experience investigating the diversion of U.S.
4 origin good to prohibited destinations, the UAE is a known diversion point, in part
5 because of Free Trade Zones that are meant to facilitate rapid movement of goods.
6 Karupini Holding BV, a Netherlands entity, benefits from a more favorable treatment
7 from the United States on export controls. As discussed in paragraph 10, items controlled
8 under the Commerce Control List may have a different licensing requirement depending
9 on the country of destination. The country of destination is meant to be the ultimate
10 consignee or end-user country, not the country of an intermediary or reseller . The
11 favorable treatment of Netherlands entities, which includes license exceptions² or no
12 license requirement on controlled items, is meant to facilitate legitimate trade among
13 allies with similar export control systems. By using Karupini Holding BV or De Geetere,
14 the parties in the agreement could avoid scrutiny and conceal the real end-users while at
15 the same time obtaining access to goods that otherwise may have required an export
16 license to be exported to Russia or be prohibited to be exported to Russia.

17 56. Another example of the De Geetere brothers' collaboration or coordination
18 on business is on the potential purchase of the accelerometers subject to this
19 investigation. For example, during the summer of 2022, as mentioned in paragraph 40,
20 De Geetere was attempting to buy thousands of units of the accelerometers. In order to
21 finance the purchase, the user of SUBJECT EMAIL ACCOUNT 1 reached out to the user
22 of SUBJECT EMAIL ACCOUNT 6, requesting funding to purchase accelerometers. The
23 user of SUBJECT EMAIL ACCOUNT 6, the user (whom we believe to be Tom De
24 Geetere) responded that he could not provide all 960,000 Euros needed to finance the
25 transaction. The user then suggested that De Geetere split the order in four, and that the
26 user could provide an initial 160,000 Euros to finance the order. While it is not clear if

27
28 ² License exceptions are explicit authorizations that allow for the export or reexport under stated conditions for specific items controlled under the Export Administration Regulations.

1 Tom knew about the particulars of these orders or the export control requirements for the
2 accelerometers, it is evident from this exchange and the other ones described above that
3 the brothers work closely together and leverage their businesses.

4 57. The analysis of the initial search warrant also shows, on another occasion,
5 De Geetere using ETT (Tom De Geetere's business) to buy export-controlled equipment
6 from Switzerland under a Swiss export license that was apparently obtained under false
7 pretenses for a purported end-user in the Netherlands. This equipment, it appears, was
8 intended to be illicitly diverted to China. On February 2021, De Geetere began
9 communicating with a company located in Switzerland to acquire a radio signal data
10 decoder. This equipment is controlled for export purposes in Switzerland. Based on the
11 emails, it appears the Swiss company obtained an export license, 8035432, issued by the
12 State Secretariat for Economic Affairs (SECO), to export 5 units of this equipment to De
13 Geetere for the use of the Flemish Government. The emails reveal that De Geetere
14 provided false end-user information, because he later exported the equipment to a
15 company located in Hong Kong, China via the Netherlands, and so did not provide the
16 products to the Flemish Government as he represented. During transit some of the cards
17 got damaged, however the Swiss company apparently discovered De Geetere's diversion
18 (it is unclear how) and sent an email to SUBJECT EMAIL ACCOUNT 1 that reads in
19 part, "... We have proof that your company BV KHSCM violated the Export Check Law
20 with the delivery of the 5 pcs [data decoder] cards". The company later advised them that
21 KHSCM was banned from buying more. The emails further indicate that the Hong Kong
22 customer for these data decoders still needed to replace the damaged cards, and, in an
23 apparent attempt to try to salvage this and future deals, on September 29, 2021 wrote to
24 SUBJECT EMAIL ACCOUNT 1: "Hans, as a friend, my suggestion is, ETT
25 company/You pls run this order ASAP for 3pcs [data decoder]...". Invoice and shipping
26 labels found in SUBJECT EMAIL ACCOUNT 1 appears to show De Geetere acted upon
27 that advice. Invoice 2021-10040 dated October 5, 2021, was addressed to ETT BV, with
28 export license number 8037908, with end-user listed as End user: Rijkswaterstaat Zee en

1 Sluizen Zuid, Kennedeylaan 1, Postbus 2232, 3500 Utrecht, Nederlande. The ETT
 2 employee was identified as Dick Bosh, info@ettbv.com. Thus, an employee from ETT
 3 and an ETT email address are identified in the commercial invoice.

4 58. Given the apparent collaboration between the brothers or intermixing of
 5 their businesses, I believe additional documents and emails exist on SUBJECT EMAIL
 6 ACCOUNT 6, on top of the emails and documents exchanged between SUBJECT
 7 EMAIL ACCOUNTS 1 and 6 that are contained in SUBJECT EMAIL ACCOUNT 1.
 8 (Moreover, there is probable cause to believe the already-identified emails and records
 9 still exist in SUBJECT EMAIL ACCOUNT 6, and those duplicate copies are themselves
 10 evidence of potential criminal violations, insofar as they prove the emails in SUBJECT
 11 EMAIL ACCOUNT 1 were actually communicated.) For example, the user of SUBJECT
 12 EMAIL ACCOUNT 6 may have communicated with others in his company, or with his
 13 bank, to facilitate the transfers of funds described in the communications with De Geetere
 14 (using SUBJECT EMAIL ACCOUNT 1). It is likely that the emails and documents in
 15 SUBJECT EMAIL ACCOUNT 6 surrounding the transactions discussed with De Geetere
 16 will help to provide additional details regarding those transactions. In addition, for those
 17 procurements where De Geetere was or is acting on behalf of his brother's company,
 18 records in SUBJECT EMAIL ACCOUNT 6 will potentially identify the real end-user.

19 59. *kimb@khscm.be*, **SUBJECT EMAIL ACCOUNT 7**. Based on the emails
 20 contained in SUBJECT EMAIL ACCOUNT 1, this email account appears to be managed
 21 by a person named Kimberly Beun (K.Beun), I personally confirmed with Belgium
 22 authorities that Kimberly Beun a natural Belgium person. On May 18, 2022, De Geetere
 23 received an email from SUBJECT EMAIL ACCOUNT 7 titled "Inbouw 204/KH/2022
 24 Lantana". The email had no relevant text but contained an attachment identified as
 25 "204KH2022.pdf." The attachment was an invoice to an Israeli Company for 248
 26 accelerometers valued at \$49,600. SUBJECT EMAIL ACCOUNT 7 is also copied on
 27 other emails sent to SUBJECT EMAIL ACCOUNT 1 concerning new shipping
 28 coordination (as shown in paragraph 58) and business registration, and the user of the

1 account also appears to perform other administrative functions for KHSCM. Because
 2 SUBJECT EMAIL ACCOUNT 7 is involved in creating or transmitting invoices of
 3 transactions related to diversion of U.S.-origin items, I believe more email
 4 communications and documents of evidentiary value will be found in SUBJECT EMAIL
 5 ACCOUNT 7.

6 60. double_mu2016@outlook.com, **SUBJECT EMAIL ACCOUNT 9**. The
 7 emails contained in SUBJECT EMAIL ACCOUNT 1 include a series of emails with
 8 encrypted content where an individual, going by the alias of “John Smith” and using
 9 SUBJECT EMAIL ACCOUNT 9, appears to place orders with De Geetere. The emails
 10 begin in October 2021 and continue through 2022. On February 4, 2022, Frank Smit,
 11 from L&A Freight, a Dutch company, asks De Geetere for the contact information for the
 12 “Hopsky Klant” (which open-source translation tools translates to “Hopsky Client”),
 13 regarding invoice “3/DB/2021”. De Geetere responds in part by providing the email
 14 contact for Hopsky Klant as double_mu2016@outlook.com, SUBJECT EMAIL
 15 ACCOUNT 9. De Geetere also copied SUBJECT EMAIL ACCOUNT 7 on the email.
 16 L&A Freight is a warehouse used by De Geetere to store and reexport items. L&A
 17 Freight is a logistics company based in the Netherlands that offer a variety of shipping
 18 and warehousing services. According to their website, <https://www.lnafreight.nl/>, L&A
 19 has twenty years of experience in dealing with high value, high risk, high processing
 20 speed and fragile goods such as IT hardware, electronics, and smartphones. T SUBJECT
 21 EMAIL ACCOUNTS 1, 7 and 8 have exchanges with multiple apparent L&A freight
 22 email accounts and employees regarding incoming and outgoing shipments for KHSCM.

23 61. A search for invoice “3/DB/2021” revealed a procurement that in part
 24 contained U.S.-origin satellite modems, model DMD20502E. These modems are
 25 advertised by the manufacturer for Government and Military end-users. The
 26 DMD20502E is controlled under ECCN 5A002.a.1 and would require a license for
 27 government end-users in China and Hong Kong. The invoice for Hopsky contained an
 28 address in Hong Kong Flat / RM 903C 9/F, Sunbeam CTR 27, Shing Yip St, Kwun

1 Tong, Hong Kong. When purchasing the modems from a California-based company, De
2 Geetere told the California company that the items were destined for Belgium, for use in
3 universities and by the Flemish Government.

4 **G. Vladimir Kulemekov and Hans De Geetere**

5 62. Public media reports³ link De Geetere to an individual named Vladimir
6 Kulemekov. The report of an arrest of a Swedish couple, Sergei Nikolaevich Skvortsov
7 and Elena Mikhailovna Kulkova, in Sweden charged in Sweden with espionage identifies
8 the relationship and reads in part:

9 “...For several years, the only counterparty to Skvortsov's Building and
10 Data Technologies was a firm called European Technical Trading, and
11 Skvortsov regularly received payments of exactly the same size from it,
12 although the nature of these transactions was unclear. The Swedish
13 authorities suspect that the transactions were fictitious and were used to
14 siphon money from the Netherlands to Sweden. The Dutch entity was run
15 by a Belgian, Hans de Geetere... But there's more to it: both Hans de
16 Geetere and Skvortsov had close ties with Vladimir Kulemekov, who
17 openly admits his GRU⁴ past and even takes pride in it...”

18 The article goes on to show a social media post for De Geetere with Kulemekov's
19 comment under the photo of Hans de Geetere, to demonstrate they have known each
20 other for some time. A different article⁵, states that Skvortsov is accused of conducting
21 espionage within Sweden and using Sweden as a base to conduct espionage against a
22 third country (unidentified), with Kulkova being charged with being an accomplice.
23 They came to the attention of Swedish authorities allegedly because their company's

24
25 ³The Swedes: Russian couple arrested in Stockholm has ties to GRU and Swedish military intelligence, lives next
door to Skripals' poisoner, November 28, 2022, <https://theins.ru/en/politics/257348>

26 ⁴ The Main Directorate of the General Staff of the Armed Forces of the Russian Federation, formerly the Main
Intelligence Directorate, and still commonly known by its previous abbreviation GRU, is the foreign military
27 intelligence agency of the General Staff of the Armed Forces of the Russian Federation.

28 ⁵ Blackhawk Helicopters Descend Into Swedish Home to Snag Latest Russian Espionage Arrest
<https://news.clearancejobs.com/2022/11/23/blackhawk-helicopters-descend-into-swedish-home-to-snap-latest-russian-espionage-arrest/>

1 books appeared to be cooked, with the company registering a loss each year, only to be
2 revived with an infusion of “interest from investments” to make it marginally profitable.

3 63. On various emails found from the user of SUBJECT EMAIL ACCOUNT
4 1, communicates or copies an individual named Vladimir Kulemekov. For example, in
5 email exchanges, involving SUBJECT EMAIL ACCOUNT 1, from July 1, 2022, related
6 to U.S.-origin microchips, between De Geetere and a Turkey-based logistic company, the
7 Turkish party writes in part: “Please advise us invoice and packing as we know you have
8 contacted the Russian buyer too.” The commodity for this transaction is Analog Devices
9 part number HMC647ALP6E. While this product is designated EAR99, Analog Devices
10 advertises it for Electronic Warfare Receivers, Weather & Military Radar, Satellite
11 Communications and Phase Cancellation. On the cc line the following contact email
12 address was copied as “Vladimir Kulemekov <blikulen@mail.ru>”

13 64. On March 17, 2022, the user of SUBJECT ACCOUNT 1 forwarded an
14 email to Vladimir Kulemekov <blikulen@mail.ru> related to an inquiry from S7
15 Airlines, Russia. SIBERIAN AIRLINES D/B/A S7 AIRLINES was added to the Denied
16 Parties list on June 2022 for engaging in conduct prohibited by the EAR by operating
17 multiple aircraft subject to the EAR and classified under ECCN 9A991.

18 **H. Temporary Denial Order**

19 65. Due to the likelihood of imminent export violations by De Geetere, BIS
20 issued a Temporary Denial Order (TDO) on August 26, 2022, suspending his export
21 privileges from the U.S. for six months. In an attempt to discredit the allegations in the
22 TDO, De Geetere has been contacting me directly at my official government email using
23 SUBJECT EMAIL ACCOUNT 1. In December 2022, based on these communications to
24 me, De Geetere appears to have purchased additional accelerometers, allegedly from a
25 party in China, to prove he is not the one sending them to China and provided our office
26 with the serial numbers and pictures.

27 66. De Geetere is not the only party or route being investigated by my office
28 for the diversion of accelerometers to China. However, De Geetere’s purchase

1 demonstrates his continued access to channels where the accelerometers are being sold.
2 Thus, I believe new emails will be found on SUBJECT EMAIL ACCOUNT 1 that will
3 reveal more information about those channels. In addition, De Geetere's hostile and
4 overt reaction to the Temporary Denial Order makes it likely that he is communicating
5 using SUBJECT EMAIL ACCOUNT 1 with others, perhaps including his brother or
6 other associates, regarding the Temporary Denial Order or its effects on his ability to
7 source certain U.S.-origin commodities. Law enforcement believes De Geetere remains
8 unaware that law enforcement has reviewed emails from SUBJECT EMAIL ACCOUNT
9 1, making it more likely he would have continued using that account.

10 **I. Nature of documents sought and background regarding email services**

11 67. The domain outlook.com is owned and managed by the Provider. The
12 domains khscm.be, hasainvest.be and ett.be are registered with Combell Network, a
13 Belgium company. However, an email trace conducted using open-source online tools
14 shows that the mail exchange server for the three domains routes via
15 "[domain].mail.protection.outlook.com". Outlook.com is a service from Microsoft
16 Corporation, the Provider. Based on my training and experience, companies like
17 Combell Network provide a variety of web services for a fee. On their website, Combell
18 Network discusses the range of services provided, which include website hosting services
19 and email hosting services. One of the email options offered by Combell Network is
20 Microsoft 365, "An all-in-one package, including a mailbox, Office software, 1 TB of
21 online storage, web meetings..." Based on my training and experience, Combell Network
22 will resell and obtain payment for Microsoft 365 service, but the user would complete the
23 registration and use the Microsoft 365 services via Microsoft's servers. Combell Network
24 does offer Exchange mailboxes on their own servers in Belgium for an additional fee.

25 68. A DNS 'mail exchange' (MX) record directs email to a mail server. The
26 MX record indicates how email messages should be routed. The 'priority' numbers
27 before the domains for these MX records indicate preference; the lower 'priority' value is
28 preferred. For example, the domain hostbeta might have a priority of 10, and the domain

1 hostdelta might have a priority of 20; in that scenario, the server would always try
2 hostbeta first because 10 is lower than 20. In the event of a message send failure, the
3 server would revert to hostdelta. For example, the email trace for the domain khscm.be
4 revealed a priority of “0” for server “khscm-be.mail.protection.outlook.com”. After
5 consultation with another colleague that have received additional forensic training with
6 respect to mail exchanges, we concluded that “khscm-be.mail.protection.outlook.com” is
7 an Outlook server and that the MX record priority of “0” for this domain indicates the
8 highest priority server to which email will go first, and that other MX records with higher
9 numbers, which also appeared in the open-source trace, represent backup servers.

10 69. Further, this MX analysis is further validated by the Provider’s production
11 of records for the previously authorized search warrant on SUBJECT EMAIL
12 ACCOUNT 1—which production itself demonstrated that Provider was the custodian of
13 records associated with that ACCOUNT, and so likely is for the other SUBJECT EMAIL
14 ACCOUNTS identified herein.

15 70. A preservation order was served on the Provider for the SUBJECT EMAIL
16 ACCOUNT 3,5 and 9 on August 19, 2022 on The Provider acknowledged the request on
17 September 16, 2022.

18 71. Based on my training and experience with other email providers, when the
19 subscriber sends an email, it is initiated at the user’s computer, transferred via the Internet
20 to the Provider’s servers, and then transmitted to its end destination. Depending on the
21 level of service paid for by the user, a copy of the email will be saved on the virtual
22 private server or a dedicated server. Unless the sender of the e-mail specifically deletes
23 the e-mail from the Provider’s server, the email can remain on the system indefinitely.
24 Even if the sender deletes the email, it may continue to be available on Provider’s servers
25 for a certain period of time.

26 72. A sent or received email typically includes the content of the message,
27 source and destination addresses, the date and time at which the email was sent, and the
28 size and length of the email. If an email user writes a draft message but does not send it,

1 that message may also be saved by the Provider's server but may not include all of these
2 categories of data.

3 73. In general, email hosting companies' providers like the Provider, even with
4 their service is sold by a third party, would obtain certain personal identifying
5 information when entering into a service contract. This information can include the
6 subscriber's full name, physical address, telephone numbers and other identifiers,
7 alternative e-mail addresses, and, for paying subscribers, means and source of payment
8 (including any credit or bank account number). Even if the services original service was
9 billed by Combell Network, the user may still be able to obtain additional service directly
10 from the Provider such as upgrades in plans or new services to link to its Microsoft 365
11 service. In my training and experience, such information may constitute evidence of the
12 crimes under investigation because the information can be used to identify the account's
13 user or users.

14 74. Email providers typically retain certain transactional information about the
15 creation and use of each account on their systems. This information can include the date
16 on which the account was created, the length of service, records of log-in (i.e., session)
17 times and durations, the types of service utilized, the status of the account (including
18 whether the account is inactive or closed), the methods used to connect to the account
19 (such as logging into the account via the Provider website), and other log files that reflect
20 usage of the account. In addition, e-mail providers often have records of the Internet
21 Protocol address ("IP address") used to register the account and the IP addresses
22 associated with particular logins to the account. Because every device that connects to
23 the Internet must use an IP address, IP address information can help to identify which
24 computers or other devices were used to access the e-mail account.

25 75. In some cases, e-mail account users will communicate directly with an e-
26 mail service provider about issues relating to the account, such as technical problems,
27 billing inquiries, or complaints from other users. E-mail providers typically retain
28 records about such communications, including records of contacts between the user and

1 the provider's support services, as well records of any actions taken by the provider or
 2 user as a result of the communications. In my training and experience, such information
 3 may constitute evidence of the crimes under investigation because the information can be
 4 used to identify the account's user or users.

5 76. Provider also offers provides OneDrive, a cloud storage service for their
 6 business accounts. These are created for each user and contain 1TB of cloud storage per
 7 user. According to the Provider's website describing the product information,
 8 <https://www.microsoft.com/en-us/microsoft-365>, users can upload, store, or share a
 9 number of documents and online documents using Microsoft Office online applications
 10 like Word, Document or Excel. The users also have the capability, if allowed by the file,
 11 to edit the file in the cloud. Users can also upload files to OneDrive, including photos,
 12 videos, PDFs, and text documents, until they hit the storage limit. Users can set up their
 13 personal computer or mobile phone to automatically back up files to their OneDrive
 14 Account. Microsoft maintains a record of who made changes, and when, to documents
 15 edited in Microsoft Office productivity applications like OneDrive.

16 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

17 77. Pursuant to Title 18, United States Code, Section 2703(g), this application
 18 and affidavit for a search warrant seeks authorization to permit Microsoft Corporation.,
 19 and its agents and employees, to assist agents in the execution of this warrant. Once
 20 issued, the search warrant will be presented to the Provider with direction that it identify
 21 the account described in Attachment A to this affidavit, as well as other subscriber and
 22 log records associated with the account, as set forth in Section I of Attachment B to this
 23 affidavit.

24 78. I anticipate executing this warrant under the Electronic Communications
 25 Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by
 26 using the warrant to require Microsoft Corporation to disclose to the government copies
 27 of the records and other information (including the content of communications)
 28 particularly described in Section I of Attachments B. Upon receipt of the information

1 described in Section I of Attachments B, government-authorized persons will review that
2 information to locate the items described in Section II of Attachments B.

3 79. Analyzing the data contained in the forensic image may require special
4 technical skills, equipment, and software. It could also be very time-consuming.
5 Searching by keywords, for example, can yield thousands of “hits,” each of which must
6 then be reviewed in context by the examiner to determine whether the data is within the
7 scope of the warrant. Merely finding a relevant “hit” does not end the review process.
8 Keywords used originally need to be modified continuously, based on interim results.
9 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,
10 search text, and many common e-mail, database and spreadsheet applications do not store
11 data as searchable text. The data may be saved, instead, in proprietary non-text format.
12 And, as the volume of storage allotted by service providers increases, the time it takes to
13 properly analyze recovered data increases, as well. Consistent with the foregoing,
14 searching the recovered data for the information subject to seizure pursuant to this
15 warrant may require a range of data analysis techniques and may take weeks or even
16 months. All forensic analysis of the data will employ only those search protocols and
17 methodologies reasonably designed to identify and seize the items identified in Section II
18 of Attachment B to the warrant.

19 80. Based on my experience and training, and the experience and training of
20 other agents with whom I have communicated, it is necessary to review and seize a
21 variety of e-mail communications, chat logs and documents, that identify any users of the
22 subject account and e-mails sent or received in temporal proximity to incriminating e-
23 mails that provide context to the incriminating communications.

24 //

25 //

26 //

CONCLUSION

81. On the basis of my participation in this investigation and the information summarized above, I submit that there is probable cause to believe that evidence, as set forth in Attachment B to this affidavit, of violations of Export Control Reform Act 50 U.S.C. § 4819(a)(2)(A) (prohibited conduct), 50 U.S.C. § 4819(a)(2)(C) (attempt to violate the EAR), 50 U.S.C. § 4819(a)(2)(F) (false statements to the Department of Commerce), 18 U.S.C. § 1001 (false statements), and 18 U.S.C. § 554 (smuggling goods from the United States), is presently contained in the **SUBJECT EMAIL ACCOUNTS**, which are more fully described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the aforementioned accounts, described in Attachment A, for the items listed in Attachment B, and the seizure and examination of any such items found. Because the warrant will be served on Provider, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.



Jose Rodriguez, Affiant
Special Agent
U.S. Department of Commerce

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on this 24th day of February, 2023.



THE HON. BRIAN A. TSUCHIDA
United States Magistrate Judge

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Microsoft Corporation, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Microsoft Corporation. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Microsoft Corporation, and they were made by Microsoft Corporation as a regular practice; and

b. such records were generated by Microsoft Corporation's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Microsoft Corporation in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Microsoft Corporation, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature